

## Проблема захисту даних кооперативних систем спостереження повітряного простору

УДК 004.056.53

Олексій Стрельницький

*Харківський національний університет радіоелектроніки,  
olekci.strelnyskiy@nure.ua*

Основні елементи процедури контролю повітряного простору (КПП) це: аналіз повітряної обстановки та прийняття рішень. Рішення приймає особа на основі аналізу відповідним чином підготовленої інформації про стан повітряної обстановки. Правильне рішення може бути прийнято лише тоді, коли є досить повна, точна, достовірна й безперервна інформація про повітряну обстановку в зоні управління. Отже, якість прийняття рішень визначаються складом та достовірністю інформації, на основі якої особа приймає рішення. Таким чином інформація, що циркулює в системі КПП повинна бути всебічно захищена від несанкціонованого використання та можливості її перекручування.

Основним інформаційним ресурсом системи КПП є первинні та кооперативні системи спостереження (СС). Первинна СС надає дані про місцезнаходження повітряного об'єкту, тобто відповідає на запитання «де», а кооперативна СС відповідає на запитання «хто» та дозволяє отримати польотну інформацію з борту повітряного об'єкту.

Наведені СС в певній мірі можуть відчувати вплив різного роду дестабілізуючих факторів і вимагають захисту даних на етапу її отримання.

**Мета роботи** – захист даних кооперативних систем спостереження повітряного простору.

Наявність можливості несанкціонованого використання кооперативних СС яка обумовлена сигналами, які використовуються у зазначеній системі та принципами побудови СС, що розглядаються (несинхронна мережа; одноканальна система масового обслуговування з відмовами). Ця особливість викликана примітивністю використовуваного сигналу відповіді. Дійсно, у якості сигналів відповіді кооперативних СС використовуються інтервально-часові та часово-частотні коди, які утворюються декілька вузькосмуговими сигналами на одній чи двох несучих частотах, часова відстань між якими і є кодом сигналу відповіді. Використання вузькосмугових сигналів, відомих несучих частот, апріорно відомих часових розстановок імпульсів сигналу відповіді та наявність слабоспрямованої антени на повітряному об'єкті призводить до того, що ЛВ є жаданим об'єктом засобів радіотехнічної розвідки зацікавленої сторони.

Така побудова кооперативних СС виключила як часові так і просторові різниці між корисними та імітованими сигналами, що дозволило зацікавленій стороні як несанкціоноване отримання інформації від розглядаємих СС, так і подавати їх роботу імітованими сигналами потрібної інтенсивності тобто здійснювати перекручування інформації зазначених СС, що призводить до жахливих ситуацій.

В доповіді проведено оцінку скритності існуючих кооперативних СС яка

визначає можливість несанкціонованого використання зазначених СС. Наведені розрахунки показують, що виявлення сигналів відповіді сучасних літакових відповідачів типовою системою радіотехнічної розвідки не має складнощів, що указує на відсутність енергетичної скритності існуючих кооперативних СС. При цьому слід зазначити, що виявлення сигналів здійснюється за зон дії первинних СС.

Проведено оцінку імовірності одержання координатної інформації від літакових відповідачів кооперативних СС при впливі потоку сигналів запиту, утвореного сумарним потоком сигналів запиту сусідніх кооперативних СС, потоком навмисних корельованих завад зацікавленої сторони та хаотичної імпульсної завади. Аналіз розрахунків вирішення інформаційної задачі існуючими кооперативними СС показує, що можливість зацікавленої сторони подавляти кооперативні СС за рахунок несанкціонованого використання літакових відповідачів потрібної інтенсивності ставить під сумнів можливість роботи цих систем у конфліктних ситуаціях.

Дійсно, при постановці НКЗ інтенсивністю 2000 імовірність вирішення інформаційної задачі практично дорівнює 0, що призводить до перекручування інформації про ідентифікацію повітряного об'єкту.

В докладі зазначено та проведено аналіз можливості підвищення енергетичної скритності сучасних кооперативних СС за рахунок використання складних сигналів. Наведені розрахунки показують, що використання складних сигналів у якості сигналів відповіді суттєвим чином могли б підвищити енергетичну скритність кооперативних СС і, як наслідок, захищеність даних. Однак перехід до використання складних сигналів у якості сигналів відповіді призводить до розширення часової бази сигналів відповіді, яка у свою чергу призводить до збільшення часу паралізації літакових відповідачів. Збільшення ж часу паралізації літакових відповідачів призводить до зменшення імовірності вирішення інформаційної задачі розглядаємими СС.

Таким чином, використання складних сигналів у кооперативних СС дозволяє підвищити енергетичну скритність, однак при цьому суттєво погіршується імовірність вирішення інформаційної задачі зазначеними СС, що є неприпустимим. Таким чином наведені в докладі розрахунки показують протиріччя між потребою захисту даних кооперативних СС та можливістю її реалізації на відомих принципах, що породжує проблему.

В докладі розглядається один з можливих варіантів зняття вказаної проблеми захисту даних кооперативних СС який засновано на можливості зміни сигналів, що використовуються у якості сигналів відповіді без суттєвої зміни принципу побудови зазначених систем. Метод засновано на можливості використання широкосмугових сигналів у якості складових сигналів інтервально-часових кодів. Дійсно ширина смуги пропуску приймачів кооперативних СС значно більша ширини спектру сигналу відповіді, що дозволяє здійснити заміну вузькосмугових складових на широкосмугові складові зазначених сигналів відповіді.